



Security Awareness Newsletter

November 2002

Troubled by Unsolicited Email?	Security for Home Computer Users	Microsoft Information
ZIP Files Can Zap You!	McAfee Anti-Virus Software	How to Make Windows 2000 and NT 4 Passwords Nearly Uncrackable
International Computer Security Day	The Information Age's Smokey the Bear	Cyber Bytes
Security Course: Security Fundamentals	SANS/FBI Top 20 List	Useful URLs
E-Card Warning	Updated Security Policies and Procedures Manual (SPPM)	Enterprise Policies
IT Security Services Contract Awarded		

Introduction

In an effort to emphasize the importance of security issues to all staff and to promote security awareness, the GOT Division of Security Services is pleased to provide this Security Awareness Newsletter. It is hoped that the information contained herein will provide practical tips, security solutions, and job-saving techniques.

Also, as a friendly reminder, GOT staff are encouraged to familiarize themselves with all policies, manuals, and procedures which can be found at [GOT Policies and Procedures](#).

[Back to Top](#)

Troubled by Unsolicited Email?



Are you constantly bothered by unsolicited email or email that is offensive in nature? Well we have some information that may help you get a handle on this troublesome situation.


If you receive unsolicited email (particularly emails with inappropriate adult content such as porn website advertisements), you are encouraged to report this to GOT by filling out the [GOT-F012](#) Incident Reporting Form and sending it to your designated cabinet security contact.


Also, Microsoft Outlook offers several methods to filter unsolicited email from your Inbox. One method is to download the updated Outlook filters file (filters.txt) from the hyperlink below. This file is updated weekly by the GOT Division of Security Services with key phrases that are most commonly found in unsolicited email. Click [here](#) to download a zipped copy of the file.

Once downloaded, copy the file to your Microsoft Office directory, which is most commonly located in the following path – C:\Program Files\Microsoft Office\Office.

After downloading the Outlook filter file, Outlook must then be configured to automatically remove unsolicited mail from your Inbox. By following the steps below, Outlook will take any email that meets the criteria specified in the filters.txt file and move it to a Junk Email folder:

Note: The instructions below were also published in the September issue of the Security Awareness Newsletter. We have included them again in this month's newsletter for your convenience.

1. On the Outlook standard toolbar, click the Organize  button.
 2. Click on **Junk Email**.
 3. In the bulleted items for Junk and for Adult Content messages, in each of the first lists, click **move**.
 4. When you click move, the second list on each line will change from a list of colors to a list of folder destinations. You can leave the default destination Junk Email or choose Deleted Items or Other folder.
 5. Click **Turn On** to enable the feature. *(Note: When you select **Turn On** the **Turn Off** button will automatically display, which can confuse some users – be assured that the function is on.)*
- If you are receiving unsolicited emails from a particular sender, you can also configure Outlook to filter out the email addresses of senders of unsolicited email:

1. On the Outlook standard toolbar, click the Organize  button.
2. Click on **Junk Email**.
3. Click the underlined phrase **click here**.
4. In the second bulleted item, click **Edit Junk Senders** or **Edit Adult Content Senders**.
5. Click on **ADD** to add an email alias or a domain of a sender. You can also review, edit, or delete entries from the list.

[Back to Top](#)

ZIP Files Can Zap You!

Your anti-virus software may not be protecting you from corrupt ZIP email attachments. Because the ZIP file specification allows extremely long file names, many anti-virus scanners will not scan these files making it possible for viruses, worms, and other malicious code to sneak right through the scanners (which only catch ZIP files with short entry names). Interestingly, the anti-virus scanners don't assume a file is dangerous if they can't scan it – instead they choose to let it through and attach a message saying it has been scanned. So the user assumes the file is safe and opens it.



This problem lies not only with anti-virus software. Since many application programmers have reused the ZIP library code for their own software packages, many operating systems and applications can be compromised by ZIP files containing long filenames. This includes software made by Microsoft, IBM and Apple.

Of particular concern are update services for things like system software, anti-virus packages, intrusion detection systems, firewalls and other critical infrastructure systems, which tend to make heavy use of ZIP archives. Some systems install and expand ZIP files automatically that are sent by network update services, unknowingly jeopardizing the network's security.

Unfortunately, the only thing that can be done to alleviate this threat is to wait for software vendors to provide updates to users. In the meantime, check with your network administrator before opening suspicious ZIP files with extremely long names.

[Back to Top](#)

November 30 is International Computer Security Day



International Computer Security Day is a globally recognized annual event set up to inform computer users of the significance of computer security. Computer Security Day began in 1988 when the Washington, D.C., chapter of the Association for Computer Machinery (ACM) sought to bring computer-related security issues to the nation's forefront. Since that time, Computer Security Day has evolved into a world-wide event. This year's theme is Preventing Intrusion.

To celebrate this day, GOT's Division of Security Services will conduct a security awareness presentation on Wednesday, November 27, 2002. The presentation will address security-related topics such as virus protection and the importance of security alerts, as well as provide an overview of the recently updated Security Policies and Procedures Manual (SPPM).

The presentation will be held in two sessions on November 27 (morning session from 9:00-11:00 a.m. and afternoon session from 1:00-3:00 p.m.) in the Cold Harbor Training Rooms A & B. To sign up, GOT employees should contact Billie Tandy at 564-0904 or BillieJ.Tandy@mail.state.ky.us.

GOT also provides security awareness presentations to agencies upon request. To arrange a security awareness presentation for your agency, please contact Linda Robinson at 564-8715 or Linda.Robinson@mail.state.ky.us.

For more information on International Computer Security Day, please visit the following website: <http://www.computersecurityday.org/>

[Back to Top](#)

Updated Security Policies and Procedures Manual (SPPM)

GOT has recently updated the [Security Policies and Procedures Manual \(SPPM\)](#), which can be found on [GOTSource](#).

The SPPM has been developed to provide a comprehensive approach to security planning and execution to ensure that GOT managed assets (hardware, software, and data) are afforded appropriate levels of protection against destruction, loss, unauthorized access, unauthorized change, and disruption or denial of service. It is a customized and comprehensive document which contains IT security policies and procedures that are to be reviewed and practiced by all GOT employees and contractors.

Some quick security tips include:

- Always lock your workstation when you leave your area.
- Turn your PC off each day before leaving.
- Display your badge at all times.
- Notify Security Services if you lose/misplace your badge.
- Swipe your card at the Cold Harbor front door when leaving.
- Check-in/out laptops at Cold Harbor.
- Shred and/or lock confidential material.
- Report suspicious activities and incidents by completing GOT-F012.
- Protect your userID -- you are responsible for every action initiated by that account.
- Create mixed-case alphabetic and special character passwords.


Also available are [Security Policy Tip Sheets](#) for managers, software designers/developers and general staff that can be found in GOTSource.


[Back to Top](#)

Enterprise Policies

Three new Enterprise Policies were recently published and have also been included in the updated [GOT Security Policies and Procedures Manual \(SPPM\)](#). All staff should read and be familiar with all security-related Enterprise Policies. These policies can be found on [GOTSource](#).

 **[Anti-Virus Policy \(CIO-073\)](#)** - Protect all computer devices from malicious code (viruses, trojans, worms, etc.)

 **[UserID and Password Policy \(CIO-072\)](#)** - Creates a standard for the creation, use, and changing of UserIDs and passwords for all state government applications, systems and services.

 **[Secure Network Architecture Policy \(CIO-074\)](#)** - Creates secure Intranet and resource domains for state applications, services, and systems. *Note: This policy contains major changes in how technology resources are placed on the Enterprise infrastructure, effective January 2003.*

 **[Internet and Electronic Mail Acceptable Use Policy \(CIO-060\)](#)** - Provides acceptable use guidelines for state employees when using state Internet and Email resources.

[Internet/World Wide Web Publishing Standards](#) - Provides standards for state websites.

[Back to Top](#)

IT Security Services Contract Awarded

The Kentucky Finance Cabinet has recently awarded contracts to AMS (Contract # C-01056178) and Kizan (Contract # C-02348682) to provide IT security-related services to the Commonwealth. The contracts cover such services as security policy and procedure creation, penetration testing, vulnerability assessment, and other types of security solutions. These contracts can be viewed and printed in the MARS Procurement Desktop (PD) module by performing the locate function.

[Back to Top](#)

E-Card Warning

Be on the lookout for E-Cards from companies that are using electronic greeting cards as a vehicle to distribute spam. Unsuspecting users are sent an email in which they are urged to pick up an "E-Card" from a website called FriendGreetings.com.



Users must then launch an ActiveX control, which automatically sends marketing material to everyone on their Outlook contacts list. The company does mention this, but it is buried in a lengthy license agreement. Use vigilance this holiday season when opening unsolicited email and visiting non-reputable websites. That innocent E-card might just cause a mass spam outbreak.

[Back to Top](#)

Security Course: Security Fundamentals



The National Cyber Security Alliance is offering a free online course on security fundamentals. The course is a introductory-level module that focuses on general awareness of computer security related issues. If you want to learn more about computer security, [click here](#) to take this free course

[Back to Top](#)

Security for Home Computer Users

Did you know that your home computer could possibly be jeopardizing the security of the Commonwealth's networks? Yes, it's true. If you use your home PC to perform tasks such as checking your email at work or updating your calendar, you could be placing the state's networks at risk if proper security measures are not followed.

Home users that do not have up-to-date anti-virus software installed on their PCs may unknowingly introduce viruses, worms, and other malicious code into the State's networks. It is also possible for hackers to use vulnerabilities in your computer's operating system or application software to "highjack" your PC and possibly gain access to the State's networks.



Implementing the following security measures are key in thwarting such risks:

- Install anti-virus software and keep the virus signature files current (see the following article on McAfee Anti-Virus Software for information on obtaining the software).
- Keep your software updated by making sure that all fixes, patches, service packs, security rollup packages, etc. are applied for both operating system and application software. If you use a Microsoft operating system or application software [click here](#) to download software updates.
- Check your Outlook and Internet Explorer settings. For more information, check out the

article "[Configuring Privacy Settings through Internet Explorer](#)" in the September issue of the Security Awareness Newsletter.

- Set up encryption in Microsoft Outlook for private e-mail messages. For how-to details, look up "encrypting e-mail" in Outlook Help.
- Install a firewall to prevent unauthorized entry of hackers into your computer. Black Ice Defender and Zone Alarm are examples of good firewall software.
- Create strong passwords such as those recommended in the [Commonwealth's Enterprise UserID and Password Policy, CIO-072](#).
- Conduct routine security maintenance such as computer backups and applying current operating system/application patches.

[Click here](#) for more detailed information on securing your home computer as recommended by Microsoft.

[Back to Top](#)

McAfee Anti-Virus Software



If you are a GOT employee or your agency participates in the Commonwealth's McAfee Active Virus Defense Program, you may be eligible to install the anti-virus software on your home computer.

The licensing agreement that the Commonwealth has with McAfee stipulates that those employees whose agencies participate in their Active Virus Defense Program are also allowed to install McAfee VirusScan on their home computers. For more information, please contact Shawn Thomas at (502) 564-9617 or Shawn.Thomas@mail.state.ky.us.

[Back to Top](#)

The Information Age's Smokey the Bear!

The [Federal Trade Commission](#) has recently launched Dewie the Turtle, the Internet's version of Smokey the Bear. In a campaign to encourage a "culture of security", Dewie offers easy-to-understand computer security advice for home and business users. Check out Dewie on the FTC's security website.



[Back to Top](#)

SANS/FBI Top 20 List

The SANS Institute and the FBI have recently released the 20 most commonly exploited vulnerable services in Windows and Unix operating systems. The overwhelming majority of successful attacks on computer systems target one or more of these twenty services. The Top Twenty is a prioritized list of vulnerabilities that require immediate attention (Top 10 for Windows and top 10 for Unix.). For more detailed information please refer to the [SANS website](#).



There is also an automated Top Twenty scanning tool that detects these vulnerabilities. The tool can be downloaded from [The Center for Internet Security](#).

[Back to Top](#)

Microsoft Information

A Good Reason to Upgrade to IE 6

In late September, the State's Internet services were adversely affected by a Denial of Service attack (DoS) that was believed to be caused by the Opaserv worm. By applying the latest security patches to your current version of Internet Explorer, or simply upgrading to version 6, you can prevent many viruses/worms such as the Bugbear/Tanatos and Opaserv from compromising your computer. For more information on Microsoft IE security patches, please reference the following website:

<http://www.microsoft.com/windows/ie/downloads/critical/default.asp>

Microsoft released MS02-062 ("IIS cumulative patch 10/2002").

The cumulative patch fixes four new vulnerabilities: local, out-of-process ISAPIs can gain system privileges; a WebDAV request memory exhaustion DoS; '.com' file upload bypasses script checking; and cross-site scripting in the administrative pages.

FAQ and patch:

<http://www.microsoft.com/technet/security/bulletin/MS02-062.asp>

Source: Microsoft

<http://archives.neohapsis.com/archives/microsoft/2002-q4/0010.html>

Microsoft released MS02-063 ("PPTP buffer overflow").

This patch fixes the vulnerability previously discussed in {02.39.012} ("PPTP preauthorization buffer overflow").

FAQ and patch:

<http://www.microsoft.com/technet/security/bulletin/MS02-063.asp>

Source: Microsoft

<http://archives.neohapsis.com/archives/microsoft/2002-q4/0009.html>

Microsoft released MS02-064 ("Win2K root folder improper permissions").

The root drive folder (C:\) in all versions of Windows 2000 gives 'everyone' full control. Since the root directory is automatically in the path under certain situations, this could let an attacker place a trojan on the system for execution.

FAQ and patch:

<http://www.microsoft.com/technet/security/bulletin/MS02-064.asp>

Source: Microsoft

<http://archives.neohapsis.com/archives/microsoft/2002-q4/0008.html>

[Back to Top](#)

How to Make Windows 2000 and NT 4 Passwords Uncrackable

Hackers often utilize various password cracking tools to decipher passwords. There is a way, however, to make your Windows 2000/NT 4 passwords more secure -- include ASCII characters in your password. Most password cracking software have the ability to crack up to 68 of the 256 possible characters in the ASCII character set. So what about the other characters? There are 187 characters of 308 (some extra Windows characters are also allowed in passwords) that can not be cracked by password cracking software. All of these characters are ones that are only accessed by pressing ALT plus a three or four digit number on the numeric keypad. Incorporating any one of these 187 characters into your password instantly makes it extremely difficult to decipher. This doesn't mean that some time in the future there may be a tool that could check for these characters and resolve hashes for them, but for now it is a good way to create secure passwords.

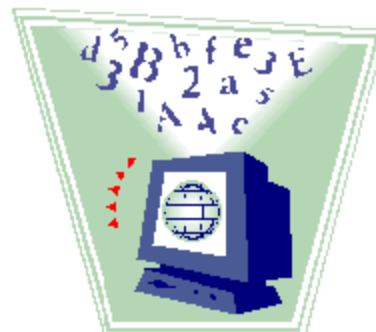


Table of Uncrackable Alt-Characters

1= ☺	21= §	143= Å	172= ¼	192= Ł	212= Ł	232= Φ	252= ŋ	177= ±	229= Å
2= ☻	22= ¯	144= É	173= ï	193= Ɔ	213= Ɔ	233= Θ	253= *	178= *	230= æ
3= ♥	23= ‡	145= æ	174= «	194= Ƨ	214= Ƨ	234= Ω	254= ■	181= μ	231= ç
4= ♦	24= †	146= £	175= »	195= †	215= †	235= ⋈	255= ⑆	182= ¶	233= é
5= ♣	25= ↓	148= Ö	176= ¶	196= −	216= ‡	236= ∞	127= 0	183= ▪	241= ñ
6= ♠	26= +	153= Ü	177= ¶	197= ‡	217= Ɔ	237= Φ	131= Ɔ	186= °	246= ö
7= ▪	27= ←	154= Ü	178= ¶	198= ‡	218= Ɔ	238= €	135= ‡	187= »	247= ÷
8= ▣	28= L	155= ¢	179=	199= ‡	219= ▣	239= Ɔ	149= ▪	188= ¼	
9= ○	29= ++	156= £	180= †	200= Ɔ	220= ▣	240= ≡	160= ⑆	189= ½	
10= ◻	30= ▲	157= ¥	181= ‡	201= Ɔ	221= ▣	241= ±	161= i	191= ¿	
11= ◊	31= ▼	158= ¢	182= ‡	202= Ɔ	222= ▣	242= ≥	162= ¢	196= Ä	
12= ♀	32= S	159= Ɔ	183= ¶	203= Ɔ	223= ▣	243= ≤	163= £	197= Å	
13= ♀	127= Δ	164= ñ	184= ¶	204= Ɔ	224= Ɔ	244= Ɔ	164= ¢	198= £	
14= ♀	128= Ç	165= Ñ	185= ¶	205= =	225= Ɔ	245= Ɔ	165= ¥	199= Ç	
15= ☺	129= Ü	166= ¢	186= ¶	206= Ɔ	226= Ɔ	246= ÷	166= !	201= É	
16= ►	130= é	167= °	187= ¶	207= Ɔ	227= Ɔ	247= ≈	167= §	209= Ñ	
17= ◄	132= ä	168= ¿	188= ¶	208= Ɔ	228= Σ	248= °	170= ¢	214= Ö	
18= †	134= Å	169= Ɔ	189= ¶	209= Ɔ	229= σ	249= ▪	171= «	220= Ü	
19= !!	135= ç	170= Ɔ	190= Ɔ	210= Ɔ	230= μ	250= ▪	172= Ɔ	223= Ɔ	
20= ¶	142= Ä	171= ½	191= Ɔ	211= Ɔ	231= Ɔ	251= √	176= °	228= ä	

Keep in mind that this covers only one small element of overall system and network security. Keystroke loggers and fast eyes can still spy on users' keystrokes to acquire passwords.

[Back to Top](#)

Cyber Bytes



Major Internet Backbone Attack Could be First of Many

The distributed denial of service (DDOS) attack launched in late October against most of the Internet domain name system (DNS) root servers failed to bring down the Internet, but that doesn't mean that more attacks won't follow and succeed where October's attack failed, according to experts, some of whom feel that the federal government needs to step in to secure the Net infrastructure.

Fortunately, the October attacks were not sophisticated, relying on a simple "packet flood" approach in which information packets are sent in high volumes to a server, and using a protocol -- ICMP -- that is typically not seen in very high volumes. more....
<http://www.itworld.com/Sec/3834/021023attacks/>

CD-ROMs for UN Inspectors Contained Viruses

UN inspectors in Vienna were given four CD-ROMs of reports from an Iraqi official; the disks also contained computer viruses. The viruses were fairly common, leading to speculation that their appearance on the disks was not intentional, but the result of inadequate anti-virus software. American companies are prohibited from exporting their products to Iraq under the current US embargo.

Chinese Computers Have High Rate of Virus Infection

The China Daily newspaper reported the results of a survey conducted by the National Computer Virus Emergency Response Center that found that 80% of computers in China are infected with viruses. Half of the infected machines had suffered data losses, problems browsing the Web, or other damage, the newspaper said. Only a small percentage of Chinese have access to computers and the Internet, but with a population of nearly 1.3 billion, the absolute numbers are still huge. China added 12 million new Internet users in the first six months of this year, pushing its total to more than 45 million, official data show.

Security Breach Causes Headaches for Microsoft

A computer security breach on a Microsoft server has forced all of the company's beta testers to change their access identification and password, and has left some wondering about Microsoft's own computer security. The intrusion happened on the server operating the Windows Beta website, commonly known as "Betaplace." Beta testers around the world routinely access programs they are evaluating by logging onto the site using Passport, Microsoft's authentication service. The Windows Beta server is the main repository for nearly all software applications undergoing beta testing that use the Windows operating system. Microsoft was unsure as to how many applications could have been compromised or how many applications or related software tools were on the server.

[Back to Top](#)

Useful URLs

The [CERT Coordination Center](#) (CERT/CC) is a center of Internet security expertise, at the Software Engineering Institute, a federally funded research and development center operated by Carnegie Mellon University. The CERT studies Internet security vulnerabilities, handles computer security incidents, publishes security alerts, researches long-term changes in networked systems, and develops information and training to help you improve security at your site.

[The Federal Computer Incident Response Center](#) (FedCIRC) is the central coordination and analysis facility dealing with computer security-related issues affecting the civilian agencies and departments of the federal government. FedCIRC's incident response and advisory activities bring together elements of the Department of Defense (DOD), Law Enforcement, Intelligence Community, Academia and computer security specialists from Federal Civilian Agencies and Departments forming a multi-talented virtual security team.

[Infosec news](#) is news service is backed by SC Magazine - the largest circulation information security magazine. It is read in more than 50 countries around the world and is published in three separate editions in North America, Europe and the Asia Pacific region. The news service gathers information globally through a network of correspondents and over 200 news services. Key links associated with the news direct you to further sources of information relevant to the news item being reported.

[Incidents.org](#) is a virtual organization of advanced intrusion detection analyst experts and forensic incident handlers from across the globe. The organization's mission is to provide real time driven security intelligence and support to both organizations and individuals.

[Computerworld](#) continually provides IT leaders with a host of targeted information services including their award-winning newspaper, web site, email newsletters, events and books. What's more, they provide unmatched reach to IT leaders with targeted advertising and sponsorships.

Located in the FBI's headquarters building in Washington, D.C., the [NIPC](#) brings together representatives from U.S. government agencies, state and local governments, and the private sector in a partnership to protect our nation's critical infrastructures. Established in February 1998, the NIPC's mission is to serve as the U.S. government's focal point for threat assessment, warning, investigation, and response for threats or attacks against our critical infrastructures. These infrastructures, which include telecommunications, energy, banking and finance, water systems, government operations, and emergency services, are the foundation upon which our industrialized society is b

[The SANS Institute](#) (System Administration, Networking, and Security) is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face.

[SearchSecurity.com](#) is the home of TechTarget, offering the most targeted media for enterprise IT professionals, including industry-specific web sites, more than 100 e-mail newsletter titles, print media, exclusive, invitation-only conferences, live online events and list rentals.

[Security Focus](#) ensures the integrity of enterprises' assets through its SIA – Security Intelligence service. SIA enables IT managers to get the latest vulnerability information as soon as it becomes available through e-mail, voice message, fax, or SMS (Small Message Service) on wireless phones. SIA provides all known information available about vulnerabilities, their causes, and severities creating actionable information to bolster computers from attack.

[ZDNet](#) operates a worldwide network of Web sites for people who want to buy, use, and learn about technology. Winner of the Computer Press Association's "Best Overall Site" award for two consecutive years, ZDNet provides an invaluable perspective and resources for technology decision makers to gain an edge in business.

[Back to Top](#)

Sources: ZDNet, the SANS Institute, Security Awareness, Inc., IT World.com, SysOpt.comand, the Federal Trade Commission.